The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/14/2009

SUBJECT:
Vulnerabilities in Microsoft .NET and Silverlight Could Lead to Remote Code Execution (MS09-061)

OVERVIEW:
Three vulnerabilities have been discovered in the Microsoft **.**NET Framework, a widely used Microsoft software development platform, which could allow an attacker to take complete control of an affected system. The **.**NET Framework is widely installed as it is a prerequisite for many common applications. These vulnerabilities can be exploited if a user visits a malicious web page or uploads a specially crafted application to an affected web server. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Microsoft Silverlight 2.0
Microsoft **.**NET Framework 1.0
Microsoft **.**NET Framework 1.1
Microsoft **.**NET Framework 2.0
Microsoft **.**NET Framework 3.5 SP1

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Microsoft .NET is Microsoft's managed code programming model for applications. Microsoft .NET consists of a common language runtime (CLR) and framework code library. Multiple remote code execution vulnerabilities have been discovered in Microsoft .NET Framework that can allow malicious Microsoft .NET applications and Microsoft Silverlight applications to execute arbitrary unmanaged code. These vulnerabilities can be exploited through several attack scenarios. In the first scenario, users can be exploited if they visit a specially crafted web site that hosts malicious XAML (Extensible Application Markup Language) content. In the second scenario, an attacker uploads malicious ASP.NET code to a web server that hosts user-created content. In the third scenario, an attacker can exploit this issue by placing a malicious .NET application on a compromised network share.

Microsoft .NET applications and Silverlight applications that are not malicious are not at risk for being compromised because of this vulnerability.

In a web server attack scenario, the attacker would gain the same privileges as the service account associated with the application pool identity. Depending on the privileges granted to the service account and on application pool configuration, an attacker might be able to take control of other application pools on the affected system. In the case of web-browsing or network share attack scenarios, successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has listed several workarounds that would prevent the vulnerabilities being exploited on affected systems prior to the patch being applied. These workarounds include disabling partially trusted .NET applications and disabling XAML browser applications in Internet Explorer. Please note that these workarounds could negatively affect business operations.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all services.
- Unless there is a business need to do otherwise, disable partially trusted Microsoft .NET applications
- Unless there is a business need to do otherwise, disable XAML browser applications in Internet Explorer

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS09-061.mspx
http://technet.microsoft.com/en-us/library/cc781986(WS.10).aspx

Security Focus:

http://www.securityfocus.com/bid/36618

Secunia:

http://secunia.com/advisories/37006/

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0090
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0091